

UNITED STATES DISTRICT COURT

for the
District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 3:25-mc-00506

Apple iPhone IMEI 359135152316007 and forensic
image, located at HSI Portland, 4310 S. Macadam Ave.
Suite 400, as described in Attachments A1 and A2

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Apple iPhone IMEI: 359135152316007 and computer forensic image of it, currently located in the HSI Portland evidence room, 4310 S. Macadam Ave., Suite 400, as described in Attachment A1 and A2.

located in the _____ District of _____ Oregon _____, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1349	Conspiracy to Commit Wire Fraud
18 U.S.C. §§ 1343, 2	Wire Fraud

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

HSI Special Agent Christopher Polinsky

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

Telephone at 12:29 pm a.m./p.m. (specify reliable electronic means).

Date: 05/02/2025

Youlee Yim You
Judge's signature

City and state: Portland, Oregon

Youlee Yim You, United States Magistrate Judge

Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF CHRISTOPHER POLINSKY

**Affidavit in Support of an Application Under Rule 41
for a Warrant to Search and Seize Evidence Including Digital Evidence**

I, Christopher Polinsky, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with Homeland Security Investigations (HSI) and have been since May 2008. My current assignment is HSI Portland Global Trade and National Security Investigations group in Portland, Oregon. While employed with HSI, I have attended numerous training courses, including the Immigration and Customs Enforcement Special Agent Training course, Criminal Investigator Training Program, and specialized courses in financial crimes, computer forensics and child exploitation investigations. I have over 16 years of experience as a law enforcement officer. As a Special Agent, I have participated in numerous investigations as either the lead case agent or as a supporting investigative agent.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of (1) Apple iPhone 12 mini with International Mobile Equipment Identification (IMEI) number: 359135152316007 (hereinafter “**Device**”) which is currently stored, in law enforcement possession, at the HSI Portland Office, 4310 S Macadam Ave., Suite 400, Portland, OR 97239, as described in Attachment A1 hereto, and (2) a computer forensic image of Apple iPhone, IMEI: 359135152316007 which is stored on forensic evidence server located in the HSI Portland, 4310 S. Macadam Ave., Suite 400, Portland, OR 97239, as described in Attachment A2, (collectively hereinafter “**Devices**”) hereto, as described in Attachment B hereto. As set

forth below, I have probable cause to believe and do believe that the items set forth in Attachment B constitute evidence contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 1349, conspiracy to commit bank fraud, and 18 U.S.C. § 1343, wire fraud.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. I believe there is probable cause to believe that evidence of the following violations will be found in the places to be searched:

- a. 18 U.S.C. §§ 1343 and 1349 make it unlawful for any individual, having devised or intended to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, and to conspire to do so.

///

///

Additional Information About Organized Retail Crime (ORC) and the Scheme to Defraud Retailers of Heavy-Duty Equipment.

5. I have conducted financial investigations involving money laundering, fraud, wire fraud, bank fraud, and identity theft, among other things. Through training and experience, I have become familiar with ORC. In general, ORC is the large-scale theft of retail merchandise with the intent to resell the items for financial gain. ORC typically involves a criminal enterprise employing a group of individuals who steal, defraud, and/or comprise a scheme to defraud large quantities of merchandise and other items of value from various stores and a fencing operation that converts the stolen and/or fraudulently obtained goods into cash. These items are often sought due to their high liquidity and value. Stolen and fraudulently obtained items are then often sold through online auction sites, at flea markets, and even to other retailers, who are often unwitting buyers.

6. This scheme generally requires the perpetrators to be in communication, which is often done via cell phone via voice communications, text messages, and other messaging applications (i.e., WhatsApp, Facebook Messenger, Signal, etc.).

7. Through HSI Special Agent (SA) Chad Lindsly's investigation in this case, I have learned that during at least 2023, The Home Depot (THD) has been the target of increased incidents involving the rental and subsequent theft of heavy-duty equipment, including dingoes, skid steers, and mini excavators. These rental incidents have had a direct and indirect financial impact on THD in excess of millions of dollars. This heavy-duty equipment is targeted because of its high value, liquidity, and ease to rent the high-valued equipment.

8. Often, in an attempt to deter ORC, heavy-duty equipment rental retailers like THD install covert tracking devices on the high-valued equipment in the event the retailer needs

to locate and recover stolen or fraudulently obtained heavy-duty equipment. In general, criminal enterprises are becoming more aware of this technique and are subsequently removing the covert tracking devices shortly after taking possession of the heavy-duty equipment. Criminal enterprises are also removing and defacing THD's markings on the equipment. These efforts are made to deter retailer and law enforcement investigation and recovery of the assets.

Additionally, based on my knowledge, training, experience, and talking to other agents, I believe the removal of the covert tracking device(s) and THD's markings by the criminal enterprise is strong evidence that the overall intent of the rental of the equipment was a scheme to defraud the retailer of the asset and not a legitimate rental.

9. Based on my knowledge, training, experience, and talking to other agents, I know that it is often common for those engaged in ORC to frequently travel to a jurisdiction(s) outside of their respective normal geographic area, i.e., where the individuals reside and frequent. This is done for several reasons. First, traveling to a different jurisdiction to commit the offense makes it more difficult to identify the perpetrator(s). Second, if a suspect(s) is positively identified, it can be difficult for one state and local law enforcement agency to investigate outside of its' respective jurisdiction and/or request support from the related jurisdiction (i.e., the crime was committed in jurisdiction A but the suspect(s) resides in jurisdiction B). Third, most of the rental incidents (i.e., the rental of a piece of heavy-duty equipment and the failure to return the equipment) are viewed as a property crime and seldomly investigated due to strained police resources, among other things. Fourth, often the recovery of the stolen and/or fraudulent obtained asset occurs in another jurisdiction (i.e., a different jurisdiction than where the perpetrator(s) resides and where the crime occurred).

Statement of Probable Cause

10. In September 2023 HSI Portland and SA Chad Lindsly initiated an investigation into a fraudulent rental / theft scheme of heavy-duty equipment from THD and the respective individuals that were directly and indirectly involved. The individuals that rented the equipment generally used their real driver's licenses, which assisted in the investigation. The purpose of the rentals was to defraud THD of the respective asset, which would be resold to an unwitting purchaser via an online platform, including at least Facebook Marketplace. The resale of the asset by the perpetrator(s) would be supported by fraudulent documents and the removal of THD's unique identifying markings on the asset. The resale value would be significantly less than the true value of the asset. This was corroborated by at least one asset located as part of the investigation.

11. SA Lindsly learned that an Asset Protection Specialist (APS) with THD was assigned to this investigation. SA Lindsly reviewed THD internal investigative reports and other work product materials, CCTV footage and still frames, police reports from various local police departments, and spoke directly with THD APS regarding the facts and circumstances around the internal fraud investigation.

12. In summary, SA Lindsly learned that THD APS had identified and linked at least 21 rentals (including one attempted) and subsequent thefts of heavy-duty equipment from more than 17 THD locations in Oregon, Washington, and California between the time period of May 23 – July 5, 2023. SA Lindsly learned that the same vehicles were used to drive away with THD's asset, the same credit card numbers were used for the rental deposits, real driver's licenses were used to rent the equipment, and CCTV still frames showed the people involved

with the rentals. Additionally, only 3 of the 20 assets have been located and/or recovered to date.

13. The rentals were conducted several different ways. First, on some occasions one member of the DCO would be the only individual present for the rental. Second, a member of the DCO would conduct the rental while being accompanied by another member of the DCO standing immediately next to the individual conducting the rental. Third, a sole member of the DCO conducted the rental; however, a review of the exterior CCTV revealed another unknown individual(s) was present driving the vehicle to assist hooking up the asset.

14. Julian Pace is believed to be a member of the DCO that is indirectly involved in a heavy-duty equipment rental / theft fraud scheme between at least May 23 – July 5, 2023. Pace has not been identified as being directly attributable to any rentals (i.e., Pace did not present his valid driver's license and/or be physically present during any of the rentals identified herein); however, a white Dodge Ram 2500 bearing Washington license plate D82366B that was rented by Pace during the same time period has been identified as the vehicle used to haul away six separate rentals. The truck was identified in CCTV footage and listed on THD's "Trailer Rental Check Out / Check In Form" as the vehicle that towed away the rented equipment. The subsequent investigation revealed that Pace had rented Pace's Rental Dodge from Enterprise Car Rental in Seattle, Washington between May 22, 2023, to June 8, 2023, and the reported total miles driven was 1,178 miles.

15. The investigation revealed that Pace uses at least one cellular phone. This phone was listed in the rental paperwork for the Dodge truck, is subscribed to Pace's former residence address, is linked to his CashApp account, and a detailed transactional analysis between Pace's

Phone and other co-conspirators revealed communications in temporary proximity to the relevant time period and specific rentals identified herein. SA Lindsly's analysis of call detail records was between at least the time period of May 1 – August 31, 2023. The communications between Pace (using Pace's Phone) and Clark (using Clark's Former Phone and Clark's VoIP Phone), Newton (using Newton's Phone), Shaw (using Shaw's Former Phone and Shaw's Phone), and McCrary (using McCrary's VoIP Phone) were consistent with Pace and other co-conspirators communicating to plan, coordinate, and execute the rental / theft fraud scheme over the course of the relevant time period.

16. On April 2, 2024, the investigation was presented to a federal grand jury which indicted Roy Lennel Clark, Lawrence Shaw, Olivia Harris, Ronald Newton, Davarian McCrary, Julian Pace, and Zipporah Myers for their involvement in the fraud scheme, case number 3:24-cr-00122-MO. Pace was charged in Counts 1 and 2 of the indictment.

17. On April 4, 2024, all seven indicted defendants were entered into the National Crime Information Center (NCIC) database as active arrest warrants.

18. On April 10, 2024, Julian Pace was arrested by Shoreline Police Department (SPD) on two outstanding warrants. A search of Julian Pace incident to arrest, revealed a black Apple iPhone (**Device**), which was detained by SPD and turned over to the South Correctional Entity (SCORE) jail then subsequently transferred to King County Correctional Facility (KCCF) in Seattle Washington.

19. On April 11, 2024, Julian Pace and his detained property were transferred from KCCF custody to HSI Seattle custody. HSI Seattle transported Julian Pace to the Federal Court House in Seattle. HSI Seattle transferred custody of Julian Pace to the U.S. Marshals for Pace's

initial appearance. HSI Seattle sent Pace's Apple iPhone (**Device**) to HSI Portland for further investigation.

20. On April 15, 2024, HSI Portland received Pace's Apple iPhone (**Device**) documented on DHS Form 6051D. I examined the Device and noted it was turned off. I also observed there were cracks in the glass on the front and back of the phone. I removed the Subscriber Identity Module (SIM) card from the **Device** and recorded the IMEI number on the tray as 359135152316007 (photo of IMEI and **Device** in Attachment A1). The IMEI number identifies the device on the mobile provider's network. HSI Portland documented the receipt and then transferred the phone (**Device**) to the evidence vault located at 4310 S Macadam Ave, Portland, Oregon 97239 .

21. On April 19, 2024, a DHS Summons was sent to AT&T Inc., identified as the mobile provider for phone number 206-617-3930 (Pace's Phone). On the same day AT&T Inc. returned information showing IMEI 359135152316007 was associated with Pace's Phone between December 20, 2023, and April 10, 2024. The AT&T Inc. return also showed the IMEI 359135152316007 is an Apple iPhone Mini. Between at least April 12, 2023, and December 20, 2023, Pace's Phone number had listed at least 2 other Apple iPhone 12s. As the AT&T Inc. return showed only Apple iPhones associated with the account, it is believed that data was copied from an old phone to the new phone on each exchange.

22. On April 19, 2024, U.S. Magistrate Judge Honorable Stacie Beckerman authorized the search of the **Device** by signing Oregon District Court search warrant 3:24-mc-435, as shown in Attachment C hereto.

23. On April 22, 2024, Computer Forensic Agent (CFA) Alex Nguyen forensically

imaged the **Device** using a combination of hardware and software. The forensic image was created using the Magnet Greykey hardware/software. The Magnet Greykey image was imported into Universal Forensic Extraction Device (UFED) Physical Analyzer. UFED Physical Analyzer is used to process the forensic image of the **Device**. CFA Nguyen used UFED to create a portable case for review. CFA Nguyen explained that because the iPhone was off before attempting the extraction, the state of the phone was known as before first unlock (BFU). In this state, data is encrypted, and certain features are restricted until the user enters the passcode.

24. I conducted a review of the portable case provided to me by CFA Nguyen. The review did not produce any information substantive to the investigation. As CFA Nguyen had already explained the state of the phone, it was reasonable to believe the substantive information was still locked in the phone.

25. Based on my training and experience, I know that new computer software and hardware are constantly being developed. I know that with new developments, some devices can be unlocked that were once considered unobtainable. Based on this knowledge, I believe that possible evidence of these violations that are currently locked in the **Device** could be obtained in the future when new digital software and hardware are developed. As the **Device** could not be unlocked, it is reasonable to believe that there may still be substantive information on the **Device**.

26. In April 2025, during a review of evidence for the case, it was discovered that the computer forensic portable case I previously reviewed was of different Apple iPhone. It is believed that the wrong file was pulled into UFED Physical Analyzer to process. Further review discovered the **Device** was forensically imaged on April 22, 2024, and still available for further

processing.

27. I therefore have probable cause to believe that a search of the iPhone seized during the arrest of Julian Paces on April 10, 2024, and the computer forensic image of that iPhone created on April 22, 2024 (**Devices**), will provide me with valuable information of the conspiracy, including evidence concerning Pace's whereabouts before, during, and after identified rentals, including in likely identifying the geographic whereabouts of where the heavy-duty equipment was likely sold to unwitting buyers. Additionally, the search of the **Devices** will assist me in confirming the identities of other unidentified members of the DCO and locations likely used to store proceeds, transaction receipts, rental contracts, paperwork documenting the sale of the assets to unwitting purchasers, and other evidence of the Subject Offenses. I believe that a search of the **Devices** will assist my investigation in understanding the context and content of communications between known and unknown members of the DCO, including text messages. A detailed toll analysis in temporal proximity to the rentals revealed communications between members of the DCO, including members that appeared to not be physically present during the rental(s). This is strong evidence that the members of the DCO were working in concert in furtherance of the Subject Offenses. I also believe that a search of the **Devices** will provide me with evidence corroborating the THD APS internal fraud investigation and HSI Portland's subsequent investigation.

28. The Apple iPhone 12 mini with International Mobile Equipment Identification (IMEI) number: 359135152316007 is currently in storage at HSI Portland's evidence room. The computer forensic image of Apple iPhone, IMEI: 359135152316007 is currently stored on a secured HSI forensic evidence server located at HSI Portland. In my training and experience, I

know that the **Devices** have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the **Device** first came into the possession of HSI Portland.

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Wireless telephone.* A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

b. *Storage medium.* A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

c. *IP address.* An Internet Protocol address (or simply “IP address”) is a

unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

d. *Internet.* The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

30. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, GPS navigation device, and access to the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.”

32. There is probable cause to believe that things that were once stored on the Device will still be stored there because, based on my knowledge, training, and experience, I know:

a. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded, deleted, or viewed via the Internet. Electronic files

downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

33. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Device because, based on my knowledge, training, and

experience, I know:

a. Data on the Device can provide evidence of a file that was once on the Device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the device at a relevant time. Further, forensic evidence on a device can show how and when the device was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access, use, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the device user. Last, forensic evidence on a device may provide relevant insight into the device user’s state of mind as it relates to the offense under investigation. For example, information on a device may indicate the user’s motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a “wiping program” to destroy evidence on the device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a computer (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

35. The initial examination of the Devices will be performed within a reasonable

amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

36. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

37. If an examination is conducted, and it is determined that the Devices do not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

38. If the Device contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

39. The government will retain a forensic image of the Device for a number of

reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

40. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

41. Based on the foregoing, I have probable cause to believe, and I do believe, that the Devices described in Attachments A1 and A2 contains evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 1349, conspiracy to commit wire fraud, and 18 U.S.C. § 1343, wire fraud, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the Devices described in Attachment A1 and A2 for the items listed in Attachment B and the seizure and examination of any such items found.

///

///

///

///


///

///

42. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Hannah Horsley. I was informed that it is AUSA Horsley's opinion that the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

By phone pursuant to Fed. R. Crim. P. 4.1
Christopher Polinsky
Special Agent, HSI

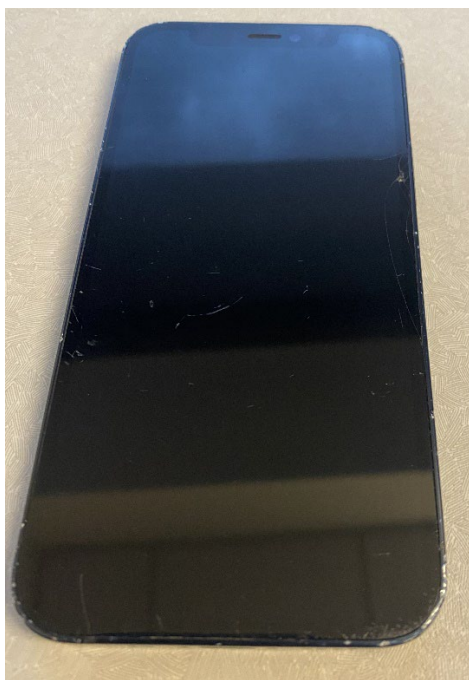
Sworn via telephone pursuant Fed. R. Crim. P. 4.1 at 12:29 pm on May 2, 2025.



HONORABLE YOULEE YIM YOU
United States Magistrate Judge

ATTACHMENT A1**Property to Be Searched**

The property to be searched is a (1) Apple iPhone, IMEI: 359135152316007 and is currently located in the HSI Portland evidence room, 4310 S. Macadam Ave., Suite 400, Portland, OR 97239.



ATTACHMENT A2

Property to Be Searched

The property to be searched is a computer forensic image of Apple iPhone, IMEI: 359135152316007 and is currently stored on a forensic evidence server located at HSI Portland, 4310 S. Macadam Ave., Suite 400, Portland, OR 97239.

ATTACHMENT B

Items to Be Seized

1. All records on the Devices described in Attachments A1 and A2 that relate to violations of 18 U.S.C. § 1349, conspiracy to commit wire fraud, and 18 U.S.C. §§ 1343, wire fraud, and involve Julian PACE, including:
2. The items referenced above to be searched for, seized, and examined are as follows:
 - a. Records or information relating to The Home Depot (THD) equipment rentals, sales/transfer of THD equipment rentals, or use of THD equipment rentals.
 - b. Evidence of who used, owned, or controlled the digital device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, calls, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence.
 - c. Records or information relating to digital or physical payment for rental or sale of THD equipment including cryptocurrencies, cryptocurrency wallets, seed words, mnemonic phrases and private keys.
 - d. Evidence indicating the digital device’s user’s state of mind as it relates to the crimes under investigation.
 - e. Contextual information necessary to understand the evidence described in this attachment.
 - f. Evidence of the times the digital device was used.

g. Evidence indicating how and when the phone was accessed or used to determine the chronological context of access, use, and events relating to the crime under investigation and to the digital device user.

h. Passwords, encryption keys, and other access devices that may be necessary to access the digital devices.

i. Records of or information about Internet Protocol addresses, cellular, or Wi-Fi networks used by the phone.

3. Records evidencing the use of the Internet, including:

a. Records of Internet Protocol addresses used.

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

c. Records of data storage accounts and use of data storage accounts.

4. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

5. The examination of the Devices may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the Devices will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Devices or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Devices do not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

9. If the Devices contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

10. The government will retain a forensic image of the Devices for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

UNITED STATES DISTRICT COURT

for the
District of OregonCertified to be a true and correct
copy of original filed in this District
Dated: **04/19/2024****MELISSA AUBIN, Clerk of Court**
U.S. District Court of OregonBy: **s/F. Patterson**Pages 1 Through 6

Case No. 3:24-mc-435

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Apple iPhone IMEI: 359135152316007, currently located in
the HSI Portland evidence room, 4310 S. Macadam Ave.,
Suite 400, as described in Attachment A

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure
of the following person or property located in the _____ District of _____ Oregon

(identify the person or describe the property to be searched and give its location):

Apple iPhone IMEI: 359135152316007, currently located in the HSI Portland evidence room, 4310 S. Macadam Ave., Suite
400, as described in Attachment AI find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B hereto.

YOU ARE COMMANDED to execute this warrant on or before May 3, 2024 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to U.S. Magistrate Stacie F. Beckerman, via Clerk.

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.Date and time issued: April 19, 2024 at 3:31 p.m.

Judge's signature

City and state: Portland, Oregon

Hon. Stacie F. Beckerman, U.S. Magistrate Judge

Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return		
Case No.: 3:24-mc-435	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: _____	_____ <i>Executing officer's signature</i>	
	_____ <i>Printed name and title</i>	

ATTACHMENT A**Property to Be Searched**

The property to be searched is a (1) Apple iPhone IMEI: 359135152316007 and is currently located in the HSI Portland evidence room, 4310 S. Macadam Ave., Suite 400, Portland, OR 97239.

**Attachment A****USAO Version Rev. July 2015****Attachment C****Page 1**

ATTACHMENT B

Items to Be Seized

1. All records on the **Device** described in Attachment A that relate to violations of 18 U.S.C. § 1349, conspiracy to commit bank fraud and 18 U.S.C. § 1343, wire fraud, and involve Julian PACE, including:
2. The items referenced above to be searched for, seized, and examined are as follows:
 - a. Records or information relating to The Home Depot (THD) equipment rentals, sales/transfer of THD equipment rentals, or use of THD equipment rentals.
 - b. Evidence of who used, owned, or controlled the digital device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, calls, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence.
 - c. Records or information relating to digital or physical payment for rental or sale of THD equipment including cryptocurrencies, cryptocurrency wallets, seed words, mnemonic phrases and private keys.
 - d. Evidence indicating the digital device’s user’s state of mind as it relates to the crimes under investigation.
 - e. Contextual information necessary to understand the evidence described in this attachment.
 - f. Evidence of the times the digital device was used.

- g. Evidence indicating how and when the phone was accessed or used to determine the chronological context of access, use, and events relating to the crime under investigation and to the digital device user.
- h. Passwords, encryption keys, and other access devices that may be necessary to access the digital devices.
- i. Records of or information about Internet Protocol addresses, cellular, or Wi-Fi networks used by the phone.
- j. As used in this attachment, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

5. The examination of the **Device** may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the **Device** to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the **Device** will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an

extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the **Device** or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the **Device** does not contain any data falling within the ambit of the warrant, the government will return the **Device** to its owner within a reasonable period of time following the search and will seal any image of the **Device**, absent further authorization from the Court.

9. If the **Device** contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the **Device** as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the **Device** and/or the data contained therein.

10. The government will retain a forensic image of the **Device** for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.